

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1066	380/28.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/12/05 07:55
L2	318	380/29.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/12/05 08:03
L3	86	(l1 or l2) and (aes or rijndael or "advanced encryption standard")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/12/05 08:09
L4	12	l3 and (("high performance" or "high speed") with (encrypt\$3 or encipher\$3 or encod\$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/12/05 08:09
L5	17	(aes or rijndael or "advanced encryption standard") same (("high performance" or "high speed") with (encrypt\$3 or encipher\$3 or encod\$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/12/05 08:24
L6	2	"VAN BUER, DARREL J".inv.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/12/05 08:18
L7	20	(aes or rijndael or "advanced encryption standard") same (pipeline with (encrypt\$3 or encipher\$3 or encod\$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/12/05 08:25


[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [Local](#) [New!](#) [more »](#)

rijndael "high speed implementation" aes pipel

[Search](#)
[Advanced Search](#)
[Preferences](#)
WebResults 1 - 10 of about 20 for rijndael "**high speed implementation**" aes pipeline. (0.77 seconds)**[PDF] Minimum Area Cost for a 30 to 70 Gbits/s AES Processor**File Format: PDF/Adobe Acrobat - [View as HTML](#)

the **AES** algorithm because **pipeline** registers will appear. inside of the byte substitution phase ... Gbits.sec, 56 mW non-pipelined **Rijndael AES** Encryption ...
www.ee.ucla.edu/~ahodjat/AES/hodjata_isvlsi.pdf - [Similar pages](#)

[PDF] Architectures and VLSI implementations of the AES-proposal ...

File Format: PDF/Adobe Acrobat

values are unacceptable for a **high-speed implementation** ... sec VLSI Implementation of the **AES Rijndael** Algorithm," Proc. CHES. 2001, May 2001. ...
dx.doi.org/10.1109/TC.2002.1146712 - [Similar pages](#)

[PDF] Microsoft PowerPoint - tut6-hsn-print1.pptFile Format: PDF/Adobe Acrobat - [View as HTML](#)

n **pipeline** stage delays over b blocks (parallel speedup) ... **Rijndael** algorithm chosen by competition. – **high-speed implementation** was one criteria ...
www.sterbenz.org/jpgs/tutorials/hsn/tut6-hsn-print.pdf - [Similar pages](#)

[DOC] HARDWARE ARCHITECTURE AND VLSIMPLIMENTATION OFFile Format: Microsoft Word 2000 - [View as HTML](#)

The combination of security, and **high speed implementation**, makes it a very ...
 B. Gladman, □The **AES** Algorithm (**Rijndael**) in C and C++, performance of the ...
www.hipc.org/hipc2004/posters/uma.doc - [Similar pages](#)

[PDF] VEST Performance Survey

File Format: PDF/Adobe Acrobat

encryption and decryption operations in one **pipeline**, advanced masking techniques ... for FPGA implementation of the **AES Rijndael** very well suited for small ...
eprint.iacr.org/2005/415.pdf - [Similar pages](#)

[PDF] A VLSI Architecture for Rijndael, the Advanced Encryption Standard ...File Format: PDF/Adobe Acrobat - [View as HTML](#)

... Rijmen as a candidate algorithm for the **AES** [27]. **Rijndael** algorithm is a round-based symmetric block cipher, which provides an ...
purl.fcla.edu/fcla/etd/SFE0000163 - Supplemental Result - [Similar pages](#)

[PDF] The Achterbahn Stream CipherFile Format: PDF/Adobe Acrobat - [View as HTML](#)

The Achterbahn Stream Cipher. Berndt M. Gammel, Rainer Gottfert, Oliver Kniffler.
 Berndt.Gammel@infineon.com. Rainer.goettfert@infineon.com. Oliver. ...
cr.yip.to/mirror.dogmap.org/streamciphers/achterbahn/desc.pdf - Supplemental Result - [Similar pages](#)

论文发表热线：**AES**算法的高速实现<硕博、MBA、MPA学位论文> - [[Translate this page](#)]

A High-speed Implementation of **AES** 作者：蔡宇东 (浙江大学.电路与系统. ... 关键字：

AES算法.流水线.轮操作. Keywords: **AES** algorithm. **pipeline**. round operation ...

www.fabiao.net/esDode.asp?SLWId=7626-22k - Supplemental Result - [Cached](#) - [Similar pages](#)

[PDF] www2.nict.go.jp/tao/kenkyu/CRYPTREC/PDF/c02e_repor...File Format: PDF/Adobe Acrobat - [View as HTML](#)

Supplemental Result - [Similar pages](#)

[\[PDF\] CRYPTREC Report 2001](#)

File Format: PDF/Adobe Acrobat

... 3.3.2 Advanced Encryption Standard (AES) ···· 126 ...

<https://www.ipa.go.jp/security/enc/CRYPTREC/fy14/doc/c01e.pdf> - Supplemental Result - [Similar pages](#)

Try searching for **rijndael "high speed implementation" aes pipeline** on [Google Book Search](#)

Google ►

Result Page: 1 2 **Next**




Free! Instantly find your email, files, media and web history. [Download now.](#)

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2005 Google

[Sign in](#)

	Web Images Groups News Froogle Local New! more »
	<input aes="" high="" implementation\"="" pipel"="" speed="" type="text" value="rijndael \"/> <input type="button" value="Search"/> Advanced Search Preferences

Web Results 11 - 14 of about 20 for rijndael "high speed implementation" aes pipeline. (0.10 seconds)

[PDF] CRYPTREC Report 2002

File Format: PDF/Adobe Acrobat

... 5 Advanced Encryption Standard (AES) ···· 179 ...

https://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/c02e_report2.pdf - Supplemental Result - [Similar pages](#)

Architectures and VLSI Implementations of the AES-Proposal Rijndael

These values are unacceptable for a **high-speed implementation** of a cryptographic

... Especially, as the **Rijndael** introducers clarify in their **AES-Proposal** ...

doi.ieeecs.org/10.1109/TC.2002.1146712 - [Similar pages](#)

www.math.utah.edu/ftp/pub/tex/bib/cryptography.html

3536k - Supplemental Result - [Cached](#) - [Similar pages](#)

DBLP - DBLP Record

DBLP Online Catalogue, DBLP Online Catalogue. Search. Keywords, Title, Author.

Printer friendly version of this page ...

dblp.doc.ic.ac.uk/viewRecord.jsp?key=phd/Dar93 - 9k - Supplemental Result - [Cached](#) - [Similar pages](#)

In order to show you the most relevant results, we have omitted some entries very similar to the 14 already displayed.

If you like, you can repeat the search with the omitted results included.



Result Page: [Previous](#) [1](#) [2](#)

[Search within results](#) | [Language Tools](#) | [Search Tips](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2005 Google



USPTO

[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

Published before January 2002

 Terms used advanced encryption standard high speed pipeline aes rijndael

Found 7 of 123,621

Sort results by

Display results

☒ Save results to a Binder

☒ Search Tips

☐ Open results in a new window
Try an [Advanced Search](#)Try this search in [The ACM Guide](#)

Results 1 - 7 of 7

Relevance scale ☐ ☐ ☐ ☐ ☐

1 [Fast implementations of secret-key block ciphers using mixed inner- and outer-round](#)

[pipelining](#)

Pawel Chodowiec, Po Khuon, Kris Gaj

 February 2001 **Proceedings of the 2001 ACM/SIGDA ninth international symposium on Field programmable gate arrays**

Publisher: ACM Press

Full text available: pdf(691.29 KB)

 Additional Information: [full citation](#), [abstract](#), [references](#), [citings](#), [index terms](#)

The new design methodology for secret-key block ciphers, based on introducing an optimum number of pipeline stages inside of a cipher round is presented and evaluated. This methodology is applied to five well-known modern ciphers, Triple DES, Rijndael, RC6, Serpent, and Twofish, with the goal to first obtain the architecture with the optimum throughput to area ratio, and then the architecture with the highest possible throughput. All ciphers are modeled in VHDL, and implemented using Xilinx ...

Keywords: AES, fast architectures, pipelining, secret-key ciphers

2 [An FPGA implementation and performance evaluation of the Serpent block cipher](#)



A. J. Elbirt, C. Paar

 February 2000 **Proceedings of the 2000 ACM/SIGDA eighth international symposium on Field programmable gate arrays**

Publisher: ACM Press

Full text available: pdf(674.09 KB)

 Additional Information: [full citation](#), [abstract](#), [references](#), [citings](#), [index terms](#)

With the expiration of the Data Encryption Standard (DES) in 1998, the Advanced Encryption Standard (AES) development process is well underway. It is hoped that the result of the AES process will be the specification of a new non-classified encryption algorithm that will have the global acceptance achieved by DES as well as the capability of long-term protection of sensitive information. The technical analysis used in determining which of the potential AES candidates will be selected as the ...

Keywords: FPGA, VHDL, algorithm-agility, block cipher, cryptography

3 [Architectural support for fast symmetric-key cryptography](#)



Jerome Burke, John McDonald, Todd Austin

 November 2000 **ACM SIGOPS Operating Systems Review , ACM SIGARCH Computer Architecture News , Proceedings of the ninth international conference**

on Architectural support for programming languages and operating systems ASPLOS-IX, Volume 34 , 28 Issue 5 , 5

Publisher: ACM Press

Full text available:  pdf(160.25 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The emergence of the Internet as a trusted medium for commerce and communication has made cryptography an essential component of modern information systems. Cryptography provides the mechanisms necessary to implement accountability, accuracy, and confidentiality in communication. As demands for secure communication bandwidth grow, efficient cryptographic processing will become increasingly vital to good system performance. In this paper, we explore techniques to improve the performance of symmetric ...

4 CryptoManiac: a fast flexible architecture for secure communication

 Lisa Wu, Chris Weaver, Todd Austin
May 2001 **ACM SIGARCH Computer Architecture News , Proceedings of the 28th annual international symposium on Computer architecture ISCA '01**, Volume 29 Issue 2

Publisher: ACM Press

Full text available:  pdf(836.04 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The growth of the Internet as a vehicle for secure communication and electronic commerce has brought cryptographic processing performance to the forefront of high throughput system design. This trend will be further underscored with the widespread adoption of secure protocols such as secure IP (IPSEC) and virtual private networks (VPNs).

In this paper, we introduce the CryptoManiac processor, a fast and flexible co-processor for cryptographic workloads. Our design is extreme ...

5 Concurrent error detection of fault-based side-channel cryptanalysis of 128-bit symmetric block ciphers

 Ramesh Karri, Kaijie Wu, Piyush Mishra, Yongkook Kim
June 2001 **Proceedings of the 38th conference on Design automation**

Publisher: ACM Press

Full text available:  pdf(260.32 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Fault-based side channel cryptanalysis is very effective against symmetric and asymmetric encryption algorithms. Although straightforward hardware and time redundancy based concurrent error detection (CED) architectures can be used to thwart such attacks, they entail significant overhead (either area or performance). In this paper we investigate systematic approaches to low-cost, low-latency CED for symmetric encryption algorithms based on the inverse relationship that exists between encryp ...

6 The year of DSC

 Dennis Fowler
December 2000 **netWorker**, Volume 4 Issue 4

Publisher: ACM Press

Full text available:  pdf(168.12 KB)  html(20.08 KB) Additional Information: [full citation](#), [index terms](#)

7 Quality of security service

 Cynthia Irvine, Timothy Levin
February 2001 **Proceedings of the 2000 workshop on New security paradigms**

Publisher: ACM Press

Full text available:  pdf(684.54 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

Keywords: quality of security service, quality of service, security range, variant security

Results 1 - 7 of 7

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2005 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)



Welcome United States Patent and Trademark Office

Search Results

BROWSE

SEARCH

IEEE XPLORE GUIDE

Results for "((rijndael<in>metadata) <and> (aes<in>metadata))<and> ('high speed'..."

Your search matched 8 of 1263585 documents.



A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

» Search Options

[View Session History](#)[New Search](#)

Modify Search

☐ Check to search only within this results set

 Display Format: ☒ Citation ☐ Citation & Abstract


» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

Select Article Information

- ☐ 1. **Architectures and VLSI implementations of the AES-Proposal Rijndael**
 Sklavos, N.; Koufopavlou, O.;
 Computers, IEEE Transactions on
 Volume 51, Issue 12, Dec. 2002 Page(s):1454 - 1459
 Digital Object Identifier 10.1109/TC.2002.1146712
[AbstractPlus](#) | [References](#) | Full Text: [PDF](#)(1528 KB) IEEE JNL
- ☐ 2. **AES crypto chip utilizing high-speed parallel pipelined architecture**
 Kotturi, D.; Seong-Moo Yoo; Blizzard, J.;
 Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on
 23-26 May 2005 Page(s):4653 - 4656 Vol. 5
 Digital Object Identifier 10.1109/ISCAS.2005.1465670
[AbstractPlus](#) | Full Text: [PDF](#)(568 KB) IEEE CNF
- ☐ 3. **A high speed FPGA implementation of the Rijndael algorithm**
 Sever, R.; Ismailglu, A.N.; Tekmen, Y.C.; Askar, M.; Okcan, B.;
 Digital System Design, 2004. DSD 2004. Euromicro Symposium on
 31 Aug.-3 Sept. 2004 Page(s):358 - 362
 Digital Object Identifier 10.1109/DSD.2004.1333297
[AbstractPlus](#) | Full Text: [PDF](#)(274 KB) IEEE CNF
- ☐ 4. **A high speed ASIC implementation of the Rijndael algorithm**
 Sever, R.; Ismailoglu, A.N.; Tekmen, Y.C.; Askar, M.;
 Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International
 Volume 2, 23-26 May 2004 Page(s):II - 541-4 Vol.2
[AbstractPlus](#) | Full Text: [PDF](#)(273 KB) IEEE CNF
- ☐ 5. **Implementation of AES as a CMOS core**
 Lan Liu; Luke, D.;
 Electrical and Computer Engineering, 2003. IEEE CCECE 2003. Canadian Co
 Volume 1, 4-7 May 2003 Page(s):53 - 56 vol.1
[AbstractPlus](#) | Full Text: [PDF](#)(357 KB) IEEE CNF
- ☐ 6. **Unlocking the design secrets of a 2.29 Gb/s Rijndael processor**
 Schaumont, P.R.; Kuo, H.; Verbauwhede, I.M.;
 Design Automation Conference, 2002. Proceedings. 39th
 10-14 June 2002 Page(s):634 - 639
 Digital Object Identifier 10.1109/DAC.2002.1012702
[AbstractPlus](#) | Full Text: [PDF](#)(650 KB) IEEE CNF

7. High-speed VLSI architectures for the AES algorithm

- ☐ Xinmiao Zhang; Parhi, K.K.;
Very Large Scale Integration (VLSI) Systems, IEEE Transactions on
Volume 12; Issue 9, Sept. 2004 Page(s):957 - 967
Digital Object Identifier 10.1109/TVLSI.2004.832943
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(576 KB\)](#) IEEE JNL
- ☐ 8. **A 2.29 Gbits/sec, 56 mW non-pipelined Rijndael AES encryption IC in a 1. μ m CMOS technology**
Kuo, H.; Verbaauwhede, I.; Schaumont, P.;
Custom Integrated Circuits Conference, 2002. Proceedings of the IEEE 2002
12-15 May 2002 Page(s):147 - 150
Digital Object Identifier 10.1109/CICC.2002.1012785
[AbstractPlus](#) | Full Text: [PDF\(589 KB\)](#) IEEE CNF
- 

Indexed by
 Inspec

[Help](#) [Contact Us](#) [Privacy & :](#)

© Copyright 2005 IEEE -

Day : Monday
Date: 12/5/2005

Time: 08:16:20

**PALM INTRANET****Inventor Name Search Result**

Your Search was:

Last Name = VAN BUER

First Name = DARREL

Application#	Patent#	Status	Date Filed	Title	Inventor Name
10038999	Not Issued	160	01/04/2002	Method and apparatus for high speed key expansion in a parallel pipelined implementation of, e.g., Rijndael or its subset AES, or other encryption algorithms with similar key data flow	VAN BUER, DARREL J.
10040087	Not Issued	30	04/15/2002	Method and apparatus for high speed implementation of data encryption and decryption utilizing, e.g. Rijndael or its subset AES, or other encryption/decryption algorithms having similar key expansion data flow	VAN BUER, DARREL J.
10730642	Not Issued	40	12/08/2003	Prediction of vehicle operator destinations	VAN BUER, DARREL J.

Inventor Search Completed: No Records to Display.

Search Another: Inventor

Last Name	First Name	
<input type="text" value="VAN BUER"/>	<input type="text" value="DARREL"/>	<input type="button" value="Search"/>

To go back use Back button on your browser toolbar.

Back to [PALM](#) | [ASSIGNMENT](#) | [OASIS](#) | [Home page](#)